(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－201143
（P2000－201143A）
(43)公開日　平成12年７月18日(2000.7.18)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/32 | | Ｈ０４Ｌ　9/00 | ６７３Ｂ | ５Ｂ０１７ |
| Ｇ０６Ｆ　12/14 | ３１０ | Ｇ０６Ｆ　12/14 | ３１０Ｋ | ５Ｂ０８５ |
| 15/00 | ３３０ | 15/00 | ３３０Ｃ | ５Ｊ１０４ |
| | | | ３３０Ｂ | ５Ｋ０３０ |
| Ｈ０４Ｌ　12/28 | | Ｈ０４Ｌ　11/00 | ３１０Ｄ | ５Ｋ０３３ |

審査請求　有　請求項の数３　ＯＬ　（全５頁）　最終頁に続く

(21)出願番号　特願平11－692

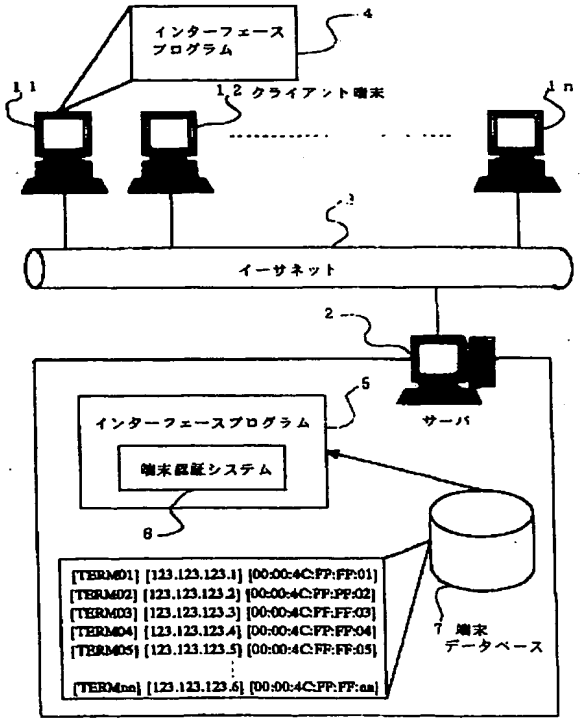
(22)出願日　平成11年１月５日(1999.1.5)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　青柳　友一
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100108578
弁理士　高橋　詔男　（外３名）

最終頁に続く

(54)【発明の名称】　端末認証装置

(57)【要約】
【課題】　クライアント端末からの不正なアクセスを阻止する機能を、サーバのプログラムのみに持たせればよい端末認証装置を提供する。
【解決手段】　サーバ２とクライアント端末１１～１ｎは、イーサネット（登録商標）３を介して接続されている。サーバ２には、クライアント端末１１～１ｎの端末名、ＩＰアドレスおよびＭＡＣアドレスからなるレコードを格納した端末データベース７を備える。また、サーバのインターフェースプログラム５には、クライアント端末１１～１ｎからの呼び出しがあると、その呼び出しプログラムからパラメータとして引き渡されるＩＰアドレスを基に端末データベース７からＭＡＣアドレスを取得し、ＩＰアドレスとＭＡＣアドレスの組み合わせが正しいか否か判定することにより、クライアント端末１１～１ｎの利用権の有無を検査する端末認証システム６を組み込んでいる。



【特許請求の範囲】

【請求項１】　ＳＯＣＫＥＴインターフェースを使用したシステムにおける端末認証装置において、

クライアント端末からの呼び出しがあると、サーバにおいて、該呼び出しプログラムからパラメータとして引き渡されるＩＰアドレスを基に前記クライアント端末のＭＡＣアドレスを取得し、ＩＰアドレスとＭＡＣアドレスの組み合わせが正しいか否か判定することにより、前記クライアント端末の利用権の有無を検査することを特徴とする端末認証装置。

【請求項２】　サーバと複数のクライアント端末とがイーサネットを介して接続されたシステムにおける端末認証装置おいて、

前記サーバには、前記クライアント端末の端末名、ＩＰアドレスおよびＭＡＣアドレスからなるレコードを格納した端末データベースを備えるとともに、

前記サーバのインターフェースプログラムにのみ、前記クライアント端末からの呼び出しがあると、該呼び出しプログラムからパラメータとして引き渡されるＩＰアドレスを基に前記端末データベースからＭＡＣアドレスを取得し、ＩＰアドレスとＭＡＣアドレスの組み合わせが正しいか否か判定することにより、前記クライアント端末の利用権の有無を検査する端末認証システムを組み込んだことを特徴とする端末認証装置。

【請求項３】　前記端末データベースのレコードに、ユーザＩＤとパスワードを付加し、前記端末認証システムは、利用者認証をも行うことを特徴とする請求項２記載の端末認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、端末認証装置、ＳＯＣＫＥＴインターフェースを使用したシステムにおいて、接続してきたクライアント端末のＩＰアドレスとＭＡＣアドレスの組み合わせによって、当該端末の正当性（利用権の有無）を検査するシステムに関する。

【０００２】

【従来の技術】従来のこの種の技術として、特開平６－３３４６７１公報に記載された「ローカルエリアネットワーク監視システム」を挙げることができる。この技術は、衝突検出型搬送波多重アクセス（ＣＳＭＡ／ＣＤ）を用いるイーサネット（ethernet）等のローカルエリアネットワークのセグメントに接続された複数の端末の各々には、それぞれ、たとえばＩＰアドレスおよびＭＡＣアドレスおよび端末名などからなる識別情報を付与して記憶しておくとともに、ネットワーク監視装置の記憶手段には、各端末の識別情報を記憶させておく。そして、端末の電源投入時に、当該端末に関する識別情報を含み、ネットワーク環境を立ち上げたことを示すブロードキャスト信号がセグメントに発行され、ネットワーク監視装置は、このブロードキャスト信号を受信すると、ネットワーク監視装置内の記憶手段の識別情報を検索し、照合する。この時、記憶手段内に受信した当該端末の識別情報が存在する場合には、当該端末のセグメントに対するするアクセスを黙認し、特に何も行わない。一方、記憶手段内に当該識別情報が存在しないと判明した場合には、制御論理が自動的に当該端末に対して衝突信号を発行し、当該端末によるＬＡＮの利用を阻止し、必要に応じて、利用を阻止した端末に関する識別情報を印字出力するなどの操作を行う。

【０００３】

【発明が解決しようとする課題】しかしながら、上述した従来技術では、ネットワーク監視装置（サーバ）側のプログラムと、端末（クライアント）側のプログラムの双方で、ＩＰアドレス、ＭＡＣアドレス、端末名などの端末の識別情報と、この識別情報を送受信するためのインターフェースを備える必要があるという問題点がある。本発明は、この点に鑑みなされたものであり、クライアント端末からの不正なアクセスを阻止する機能をサーバのプログラムにのみ持たせればよい端末認証装置を提供することを目的とする。

【０００４】

【課題を解決するための手段】そのために、第１の本発明の端末認証装置は、クライアント端末からの呼び出しがあると、サーバにおいて、該呼び出しプログラムからパラメータとして引き渡されるＩＰアドレスを基に前記クライアント端末のＭＡＣアドレスを取得し、ＩＰアドレスとＭＡＣアドレスの組み合わせが正しいか否か判定することにより、前記クライアント端末の利用権の有無を検査する。また、第２の本発明の端末認証装置は、サーバと複数のクライアント端末とがイーサネットを介して接続されたシステムにおける端末認証装置おいて、前記サーバには、前記クライアント端末の端末名、ＩＰアドレスおよびＭＡＣアドレスからなるレコードを格納した端末データベースを備えるとともに、前記サーバのインターフェースプログラムにのみ、前記クライアント端末からの呼び出しがあると、該呼び出しプログラムからパラメータとして引き渡されるＩＰアドレスを基に前記端末データベースからＭＡＣアドレスを取得し、ＩＰアドレスとＭＡＣアドレスの組み合わせが正しいか否か判定することにより、前記クライアント端末の利用権の有無を検査する端末認証システムを組み込んだことを特徴とする。本発明では、サーバ側に端末認証システムを組み込むことにより、ＳＯＣＫＥＴインターフェースを使用したシステムで利用権のないクライアント端末が、ＩＰアドレスを不正に変更し、恰も利用権のある端末に見せて不正なアクセスをすることを防止する。これは、システム内で固有のユーザＩＤ／パスワードの仕組みを用いて行うことが通例であるが、従来は、クライアント側のプログラムとサーバ側のプログラムとにその機能を持たせなければならなかった。しかし、本発明では、サー

バのプログラムにのみ端末認証システムを持つことで端末認証が可能となる。

【０００５】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。図１を参照すると、本発明の一実施例が示されており、クライアントーサーバのシステム構成で使用されることが分かる。すなわち、ｎ個のクライアント端末１１～１ｎとサーバ２とがイーサネット３を介して接続されている。各クライアント端末１１～１ｎ側には、ＳＯＣＫＥＴインターフェースプログラム４が備えられているのに対して、サーバ側２には、端末認証システム６が組み込まれたＳＯＣＫＥＴインターフェースプログラム５が備えられている。したがって、端末認証システム６は、サーバ２上にのみ存在し、サーバ側のＳＯＣＫＥＴインターフェースプログラム５に取り込まれ、１機能として動作する。また、サーバ２には、端末データベース７が設けられている。図１の端末データベース７における各レコードは、端末名、ＩＰアドレス、ＭＡＣアドレスの順番に並べられた項目からなり、各項目は、かっこ（［］）で括られて１レコードを構成する。例えば、端末名＝ＴＥＲＭ１、ＩＰアドレス＝１１１．２２２．１１１．２２２、ＭＡＣアドレス＝００：００：４Ｃ：ＦＦ：ＦＦ：ＦＦ、という端末があった場合、［ＴＥＲＭ１］［１１１．２２２．１１１．２２２］［００：００：４Ｃ：ＦＦ：ＦＦ：ＦＦ］という定義になる。ファイル形式はメンテナンスの容易性、ファイルＩ／Ｏの処理速度を考慮し、テキスト形式の順編成ファイルとする。システム運用にあたって、このようなデータが端末データベース７に予め登録されている必要がある。

【０００６】次に、図２を参照して本実施例の動作について説明する。図２は、端末認証システム６のフローチャートを示す。まず、ステップＡ１において、呼び出し元プログラムからパラメータとして引き渡されたＩＰアドレスを基に、接続相手となるクライアント端末のＭＡＣアドレスを取得する。このとき、ＡＲＰ（Ａｄｄｒｅｓｓ　ＲｅｓｏｌｕｔｉｏｎＰｒｏｔｏｃｏｌ）を使用する。ステップＡ２において、ＩＰアドレスをキーワードとして、端末データベース７を検索する。端末データベース７に該当するＩＰアドレスが存在するか、どうか判定し（ステップＡ３）、存在しなかった場合は呼び出し元プログラムにＮＧを返却し、プログラムを終了する（Ａ７）。また、ステップＡ３において、目的のＩＰアドレスが存在した場合は、ＩＰアドレスとＭＡＣアドレスの組み合わせが正しいかどうかを判定し（ステップＡ４）、判定の結果正当な端末でなかった場合は呼び出し元プログラムにＮＧを返却し（Ａ７）、プログラムを終了する。一方、正当な端末であった場合は呼び出し元プログラムにＯＫを返却し（Ａ６）、プログラムを終了する。

【０００７】次に、本発明の他の実施例について説明する。図３を参照すると、この実施例では、端末データベース９におけるレコードは、ユーザＩＤ、パスワードを組み合わせている点が図１における端末データベース７のレコードと異なる。これにより、端末認証と端末に対する利用者認証を行え、より信頼性の高い不正アクセス防止が可能となる。

【０００８】次に、図４を参照して本実施例の動作について説明する。図４は、図３における端末認証システム８のフローチャートを示す。まず、ステップＢ１において、呼び出し元プログラムからパラメータとして引き渡されたＩＰアドレスを基に、接続相手となるクライアント端末のＭＡＣアドレスを取得する。このとき、ＡＲＰ（Ａｄｄｒｅｓｓ　ＲｅｓｏｌｕｔｉｏｎＰｒｏｔｏｃｏｌ）を使用する。ステップＢ２において、ＩＰアドレスをキーワードとして、端末データベース９を検索する。端末データベース９に該当するＩＰアドレスが存在するか、どうか判定し（ステップＢ３）、存在しなかった場合は呼び出し元プログラムにＮＧを返却し、プログラムを終了する（Ｂ９）。また、ステップＢ３において、目的のＩＰアドレスが存在した場合は、ＩＰアドレスとＭＡＣアドレスの組み合わせが正しいかどうかを判定し（ステップＢ４）、判定の結果正当な端末でなかった場合は呼び出し元プログラムにＮＧを返却し（Ｂ９）、プログラムを終了する。ここまでの処理は、図２における処理と同一である。図２と図４では、共に端末データベース７または９の検索、即ちファイルＩ／Ｏは１度しか行われないため、クライアント端末１１～１ｎに対する利用者認証の機能を付け加えたとしても、処理速度に大きな影響は与えない。そこで、本実施例では、図４のステップＢ６、Ｂ７において、ユーザＩＤとパスワードの検査を行っているが、これは呼び出し元プログラムからパラメータとして与えられなければならず、そのためにはクライアント側のＳＯＣＫＥＴインターフェースプログラム４の修正も必要となる点に注意されたい。

【０００９】

【発明の効果】本システムを導入すれば、ユーザＩＤ／パスワードによる利用者認証機能を有しているシステムであれば、より信頼性の高い不正アクセス防止を実現することができるという効果を得ることができる。また、既に運用に入ってしまっているＳＯＣＫＥＴインターフェースを利用したシステムでこうした機能を有しないシステムであっても、クライアント端末側のプログラムを修正することなく、サーバ側のプログラムを修正するだけで、端末利用権の検査機能を導入することが可能である。

【図面の簡単な説明】

【図１】　本発明の一実施例のブロック図。

【図２】　図１に示した実施例における端末認証システ

ムのフローチャート。

【図３】　本発明の他の実施例のブロック図。

【図４】　図３に示した実施例における端末認証システムのフローチャート。

【符号の説明】

１１、１ｎ　クライアント端末

２、２０　　サーバ

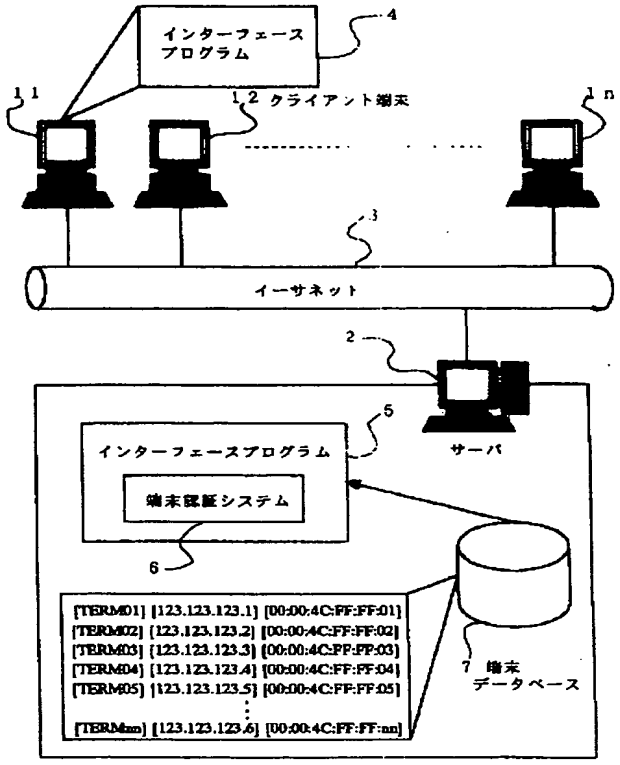
３　　イーサネット

４、５　ＳＯＣＫＥＴインターフェースプログラム

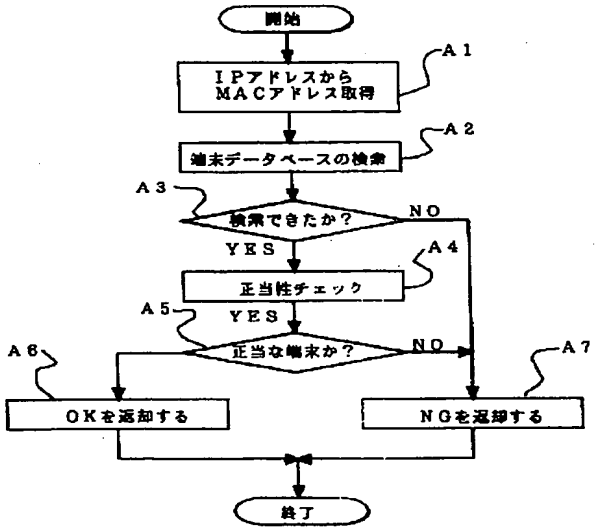
６、８　端末認証システム

７、９　端末データベース

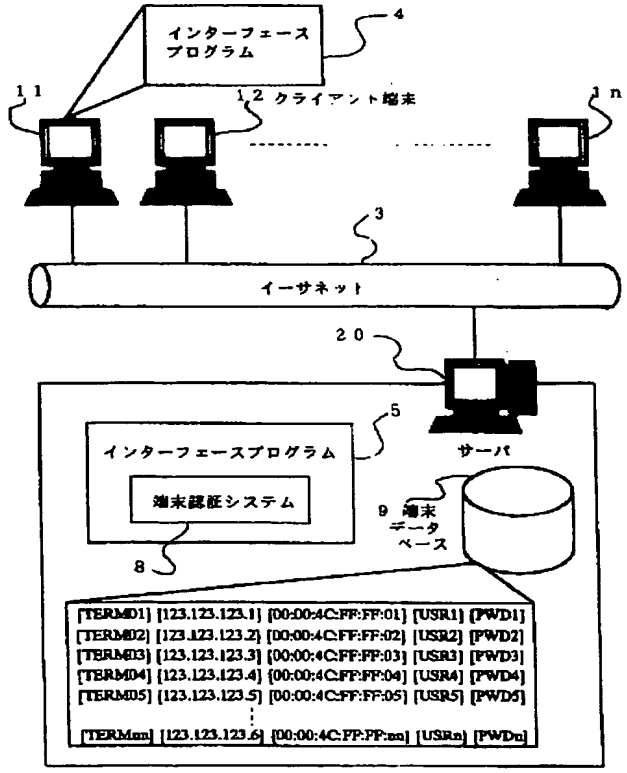
【図１】



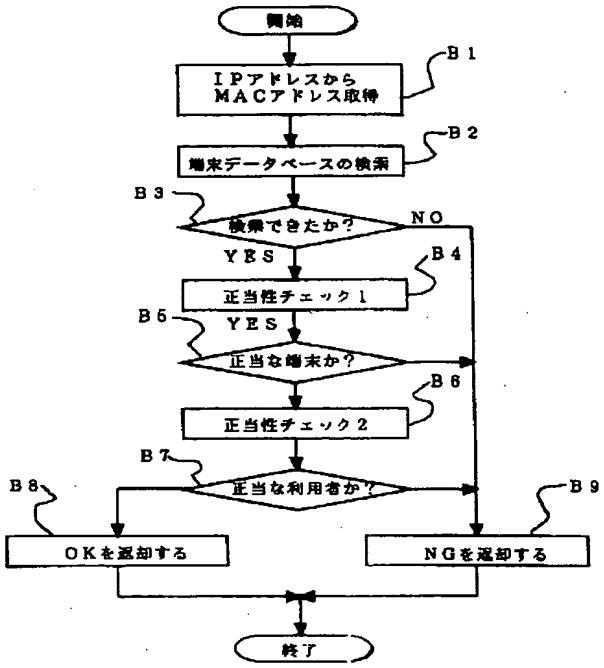

【図２】




【図３】



【図４】




フロントページの続き

| (51) Int. Cl.[7] | 識別記号 | F I | | ﾃｰﾏｺｰﾄﾞ(参考) |
|---|---|---|---|---|
| Ｈ０４Ｌ 12/56 | | Ｈ０４Ｌ 11/20 | １０２Ｚ | |

Ｆターム(参考) 5B017 AA01 BA05 BB02 BB07 CA16
5B085 AE04 AE23 BG07
5J104 AA07 KA01 KA02 NA00 NA05
NA20 PA07
5K030 GA15 HC14 HD09 JT02 JT06
LB02 LC16 LD19 LD20
5K033 AA08 CA08 CB01 DA01 DB20
EC01 EC04